

Re: Unix Bind and Windows DNS with Dynamic update issues!!!

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.dns/2005-05/msg00106.html>

- *From:* "Mugen" <Mugen@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 9 May 2005 12:52:04 -0700
-

>BTW, I use a BIND DNS server in the position that you
>suggest but it does NOT service internal clients directly.

How can i do it? If i just want Windows Clients to resolve SRV records but
still have UNIX BIND to do the rest for host name and internet resolution.
Windows 2003 DNS will acting as another internal DNS server like UNIX BIND?

BTW, We are running two BIND DNS server.... internal DNS is sitting in our
LAN and external is sitting in the DMZ zone.

>It could with views, but it would still not be holding a DIFFERENT
>set of information on the internal view than do the internal
>DNS servers responsible for maintaining the internal records
>of the domain.

"Herb Martin" wrote:

> "Mugen" <Mugen@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
> news:27734BCB-D6C0-491B-B1F5-EAD108B71CA9@xxxxxxxxxxxxxxxxxxxxx
>> Hi,
>>
>> >>DNS for AD:
>>
>> 1) Dynamic for the zone supporting AD
>> 2) All internal DNS clients NIC\IP properties must specify SOLELY
>> that internal, dynamic DNS server (set.)
>> 3) DCs and even DNS servers are DNS clients too --- see #2
>> 4) If you have more than one Domain, every DNS server must
>> be able to resolve ALL domains (either directly or indirectly)
>>
>>
>> I know it would be a "Perfect World" if i do all this.
>
> You actually have no real choice --- the above is required

Re: Unix Bind and Windows DNS with Dynamic update issues!!!

> if you wish AD authentication and replication to function
> reliably.
>
> It is also generally required to get internal DNS to work
> anyway, AD or not (except for the dynamic part.)
>
>> But the FACT is that
>> we are running UNIX BIND as internal and external DNS server.
>
> You cannot do that unless you are using Views or wish to
> expose your sensitive internal information on the Internet.
>
> That would be silly since there is practically no justifiable
> reason for doing so -- if you only can afford one server then
> your public DNS belongs at the register anyway.
>
>> All of our
>> internal clients like Windows, Mac etc are pointing to UNIX BIND server to
>> resolve internal hostname and internat name.
>
> That will only work if the BIND server has ALL of the needed
> internal names -- which mean that it is either a Dynamic Primary
> OR it is a secondary to the internal DC dynamic primary.
>
> You cannot point the clients to a server which doesn't have (and
> cannot find) all of the names they need.
>
> DNS does not work like that.
>
>> What can i do to accomplish this? I setup a Windws DNS server created 6
>> zones files in UNIX and Windows (_TCP, _UDP, MSDCS, _SITES etc) and just
> for
>> SRV records resolution. But i can only make it work if i put Windows DNS
>> server address in Windows DNS clients entrie (able to join AD Domain but
> not
>> dynamically updating clients hostanme in Windows DNS).
>
> You are working way to hard to make this more complicated
> than it needs to be -- and more fragile and less fault tolerant
> at the same time.
>
>> Can ANYONE really help with this? I am just stuck here.
>
> Yes. Do what I suggested above and in the previous post
> and it will "just work."
>
> BTW, I use a BIND DNS server in the position that you
> suggest but it does NOT service internal clients directly.
>
> It could with views, but it would still not be holding a DIFFERENT
> set of information on the internal view than do the internal

Re: Unix Bind and Windows DNS with Dynamic update issues!!!

> DNS servers responsible for maintaining the internal records
> of the domain.
>
> --
> Herb Martin, MCSE, MVP
> Accelerated MCSE
> <http://www.LearnQuick.Com>
> [phone number on web site]
>
>
>> Mugen
>>
>>
>>
>> "Herb Martin" wrote:
>>
>>> "Mugen" <Mugen@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
>>> news:D4CE1EB2-6F24-40B9-A790-B592CEA6229B@xxxxxxxxxxxxxxxxxxxx
>>>> Currently, I have a network running NT 4.0 with WINS only, but use a
> UNIX
>>> DNS
>>>> server for internal and external name resolution. The plan is to
> upgrade
>>>> to
>>>> Windows 2003/AD, but the Unix DNS server
>>>> still needs to be in place and all of our Windows clients are pointing
> to
>>>> Unix for DNS resolution. The plan is to call our new forest root
> domain
>>>> "company.com"
>>>> the same name that the Unix DNS server is the authoritative server for
> that
>>>> domain.
>>>>
>>>> You might wish to reconsider that name decision, although
>>>> I myself frequently use it. Your internal users will not be
>>>> able to address your web server using the 'base' name of the
>>>> domain (e.g., domain.com) but will require the www prefix
>>>> (e.g., www.domain.com) since all of the DCs register the
>>>> base name and interfere.
>>>>
>>>>> Now, I have setup a Windows 2003 AD and DNS test server with same FQAN
>>>>> "company.com" as UNIX (Unix is the root authoritative domain for
>>>>> "company.com"). I added Windows 2003 DNS as a thrid DNS entry in
> Windows
>>>>> clients in order for Windows clients to join AD Domain and search AD
>>>>> objects.
>>>>>
>>>>> All of your clients must use ONLY DNS servers that return a
>>>>> complete and consistent set of answers. In practice this means
>>>>> the internal DNS server set that is dynamic and support the

Re: Unix Bind and Windows DNS with Dynamic update issues!!!

>>> AD domain name.
>>>
>>>> (Otherwise Windows clients will not able to join AD Domain)
>>>
>>> Right. And will authenticate badly or not at all.
>>>
>>>> But the problem i have right now is Dynamic update is not working in
>>> Windows
>>>> DNS server unless i change the order of Windows DNS server as Primary
>>> option.
>>>
>>> Even then it will not be reliable. You must NOT depend on client
>>> "order" to make things work -- it is not reliable (nor ever intended
>>> to be reliable.) DNS clients assume that all of their DNS servers
>>> will return the SAME (and correct) answers.
>>>
>>>> Your BIND server must either be the ONLY Primary for this (internal)
>>> zone and be dynamic, or it must become a Secondary to the AD Dynamic
>>> DNS zone, or none of your internal clients may use the BIND server
>>> on their NIC client properties.
>>>
>>>> Is that true i have to make Windows client pointing to Windows DNS
> server
>>> as
>>>> Primary option in order to make dynamic update working?
>>>
>>>> No, not precisely. The above statement is an over-specific
>>> interpretation of what I wrote in the previous paragraph:
>>>
>>>> The INTERNAL clients must use strictly the INTERNAL DYNAMIC
>>> DNS servers -- no matter which machines do that.
>>>
>>>> But i really need to
>>>> have Windows clients pointing to UNIX as Primary/Secondary choice.
>>>
>>>> Why? (Truth is you do not in all likelihood need to do that.)
>>>
>>>> The internal DNS will forward to the UNIX or other DNS server
>>> to handle Internet lookups.
>>>
>>>> Whether the "BIND" server is part of that internal DNS server
>>> set is an option -- probably easiest not to do that, but still an
>>> option.
>>>
>>>> Any suggestion would be appreciate!
>>>
>>>> Completely separate your internal from your external DNS.
>>>
>>>> In fact, your external DNS is best placed back at the REGISTRAR
>>> for all but the largest (in terms of Internet presence) companies.
>>>

Re: Unix Bind and Windows DNS with Dynamic update issues!!!

>>>
>>> Here are the basic guidelines and checks to ensure with DNS for AD.
>>> (Note there is no "requirement" for removing BIND, the requirements
>>> are in terms of the functions and information of the various DNS
>>> servers.)
>>>
>>> DNS for AD:
>>>
>>> 1) Dynamic for the zone supporting AD
>>> 2) All internal DNS clients NIC\IP properties must specify SOLELY
>>> that internal, dynamic DNS server (set.)
>>> 3) DCs and even DNS servers are DNS clients too --- see #2
>>> 4) If you have more than one Domain, every DNS server must
>>> be able to resolve ALL domains (either directly or
> indirectly)
>>>
>>> netdiag /fix
>>>
>>>or maybe:
>>>
>>> dcdiag /fix
>>>
>>> (Win2003 can do this from Support tools):
>>> nltest /dsregdns /server:DC-ServerNameGoesHere
>>> <http://support.microsoft.com/kb/q260371/>
>>>
>>> Ensure that DNS zones/domains are fully replicated to all DNS
>>> servers for that (internal) zone/domain.
>>>
>>> Also useful may be running DCDiag on each DC, sending the
>>> output to a text file, and searching for FAIL, ERROR, WARN.
>>>
>>> Single Label domain zone names are a problem Google:
>>> ["SINGLE LABEL" domain names DNS 2000 | 2003 microsoft:]
>>>
>>>
>>> ---
>>> Herb Martin, MCSE, MVP
>>> Accelerated MCSE
>>> <http://www.LearnQuick.Com>
>>> [phone number on web site]
>>>
>>>
>>>
>
>
>
.

Re: Unix Bind and Windows DNS with Dynamic update issues!!!

- *Follow-Ups:*

- ◆ **Re: Unix Bind and Windows DNS with Dynamic update issues!!!**
◇ From: Herb Martin

- *References:*

- ◆ **Unix Bind and Windows DNS with Dynamic update issues!!!**
◇ From: Mugen
- ◆ **Re: Unix Bind and Windows DNS with Dynamic update issues!!!**
◇ From: Herb Martin
- ◆ **Re: Unix Bind and Windows DNS with Dynamic update issues!!!**
◇ From: Mugen
- ◆ **Re: Unix Bind and Windows DNS with Dynamic update issues!!!**
◇ From: Herb Martin

- Prev by Date: **DNS Configuration Question**

- Next by Date: **2003: "dns server unable to open active directory" (id 4000, and others)**

- Previous by thread: **Re: Unix Bind and Windows DNS with Dynamic update issues!!!**

- Next by thread: **Re: Unix Bind and Windows DNS with Dynamic update issues!!!**

- Index(es):

- ◆ **Date**
- ◆ **Thread**